METHOD AND APPARATUS FOR DETECTION OF HOSTILE SOFTWARE

ABSTRACT OF THE DISCLOSURE

Methods and apparatuses are presented for detecting hostile software in a computer system involving storing a representation of configuration data associated with an operating system for the computer system obtained at a first time, comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time, and if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained at the second time, automatically performing at least one remedial measure in response to the deviation detected. In one embodiment of the invention, the configuration data relates to identification of executable code installed in the computer system. The configuration data may be obtained from a registry key in a registry maintained by the operating system.